UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA
Case No. 20-CV-954-UA-JLW

FARHAD AZIMA,

Plaintiff,

v.

NICHOLAS DEL ROSSO and VITAL MANAGEMENT SERVICES, INC.,

Defendants.

BRIEF OF PLAINTIFF FARHAD AZIMA IN RESPONSE TO DEFENDANTS' MOTION TO DISMISS

INTRODUCTION

Defendants' motion marks their second effort to deflect their clients' criminal misconduct, and this Court's attention, from Plaintiff's Complaint, and to misdirect by repeated reference to and mischaracterization of a different case, with different claims, different operative facts, and different parties that is being litigated abroad. Defendants are attempting to create a side-show that has no bearing on this Motion. Each of Plaintiff's claims is a cognizable private right of action and contains sufficient allegations to meet the required elements, and none are time barred or subject to any preclusive effect from any prior decision.

The Complaint alleges that Defendants and others (1) procured and oversaw the hack of Plaintiff Azima's U.S. computers and email accounts as part of a conspiracy to injure him that began in 2015 and lasted for years, (2) intercepted his data and trade secrets on an on-going basis, (3) disclosed and used that data through at least June 2019, and (4)

actively concealed (and continue to conceal) their role in the conspiracy until Azima learned of their conduct in the summer of 2020.

To conceal his conduct, Defendant Del Rosso concocted a false cover story for the hack, signed a false witness statement, and provided false testimony in an English proceeding in 2020. In that proceeding, Azima's counterparty, Ras Al Khaimah Investment Authority ("RAKIA"), argued that its agents had fortuitously discovered Azima's stolen data on the internet, just in time for RAKIA to use it against Azima.

In May 2020, the English court ruled that this highly improbable "innocent discovery" story, supported by Del Rosso's testimony, was "not true" and that the "true facts" about how RAKIA obtained Azima's data "have not been disclosed." Compl. ¶ 34; ECF No. 31-2 at 116-17 ¶¶ 354-55. Azima continued to investigate and, after learning of Defendants' role in the summer of 2020, brought this lawsuit. The Complaint provides a detailed, damning narrative, stating timely causes of action that are not precluded by the English proceedings.

Tellingly, the Defendants lead arguments on their Rule 12 motion are that they are entitled to prevail on their affirmative defenses. These arguments, which are generally not appropriate at this stage, not only fail on the merits based on the face of the Complaint but also ignore the allegations of Del Rosso's actions to conceal, from both Azima and the English court, the role he played in the hacking, which is sufficient to defeat both arguments. Defendants' argument that the Complaint does not state viable claims is also without merit: the law affords remedies to a U.S. citizen whose data and trade secrets have been intercepted, disclosed, and misused.

Defendants' arguments are especially hollow at this stage of the proceedings, when the Court must determine from the face of the Complaint whether any set of plausible facts could overcome Defendants' affirmative defenses and whether Plaintiff's claims are legally viable if the alleged facts are true. The Court should deny the motion to dismiss.

ARGUMENT

I. Standard of Review

A complaint must contain sufficient factual allegations that, accepted as true, state a claim that is plausible on its face. *Edmonson v. Eagle Nat'l Bank*, 922 F.3d 535, 552 (4th Cir. 2019). The complaint "need only give the defendant fair notice of what the claim is and the grounds on which it rests." *Id.* A Rule 12(b)(6) motion "generally cannot reach the merits of an affirmative defense" under Rule 8(c), such as res judicata or the statute of limitations. *Goodman v. Praxair, Inc.*, 494 F.3d 458, 464 (4th Cir. 2007) (en banc). Such a defense may only be reached "in the relatively rare circumstances" where "all facts necessary to the affirmative defense 'clearly appear[] *on the face of the complaint.*'" *Id.* (quotations omitted).

II. Azima's Claims are Not Time-Barred.

Defendants contend that Plaintiff's claims are time-barred because the limitation period began to run in September 2016 when Azima learned that he had been hacked.[1]

[1] Seven of Plaintiff's eleven counts have three-year statutes (18 U.S.C. §§ 1831, 1832, 1836; N.C. Gen. Stat. § 14-113.20 and § 1-539.2(c); N.C. Gen. Stat. § 75-66; N.C. Gen. Stat. § 66-153 et seq.; North Carolina Common Law); one count has a four-year statute (N.C. Gen. Stat. § 75-1.1); two counts have two-year statutes (18 U.S.C. §§ 2511(1)(c) and 2520; 18 U.S.C. § 371); and one count has a one-year statute (N.C. Gen. Stat. § 14-458).

Dkt. No. 32 at 7. This argument ignores key passages of the Complaint that describe in detail the on-going misconduct, and should be rejected.

The hack was just the start of Defendants' actionable conduct. The Complaint alleges that, since 2016 and into 2020, Defendants and their co-conspirators have engaged in repeated tortious acts, including multiple disclosures and uses of Azima's data. These acts are within the limitation periods for ten of the eleven counts. Moreover, Defendants and their co-conspirators concealed their responsibility for hacking Azima and using his data for many years, tolling the statutes. Defendants cannot spend years interfering in a plaintiff's efforts to discover and timely bring a claim and then argue the plaintiff failed to timely bring those claims. We start with tolling because, if the Court finds those allegations to be sufficient, it need not consider each individual statute.

A. Defendants' Fraudulent Concealment of Their Misconduct Bars a Statute of Limitations Defense on All Counts.

The Complaint alleges that Defendants concealed their misconduct; therefore, no claims should be dismissed under the statute of limitations. Defendants cannot benefit from their own deception and claim limitations as a defense, particularly at this stage of the proceedings. Fraudulent concealment bars statute of limitations defenses for federal causes of action where (1) the defendant concealed facts that are the basis of the plaintiff's claim, and (2) the plaintiff failed to discover those facts within the statutory period, despite (3) the exercise of due diligence. *Edmonson*, 922 F.3d at 548; *Supermarket of Marlinton, Inc. v. Meadow Gold Dairies, Inc.*, 71 F.3d 119, 122 (4th Cir. 1995). Fraudulent concealment may be established through acts of co-conspirators. *See In re Refrigerant*

Compressors Antitrust Litig., 92 F.Supp.3d 652, 669 (E.D. Mich. 2015). While Plaintiff must state with particularity the circumstances constituting fraudulent concealment, a court will not dismiss a complaint when the defendant is made aware of the circumstances for which it will have to prepare a defense and the plaintiff has substantial pre-discovery evidence. *Edmonson*, 922 F.3d at 553.

Similarly, "North Carolina courts have recognized and applied the principle that a defendant . . . may be equitably estopped from using a statute of limitations as a sword, so as to unjustly benefit from his own conduct.[]" *Friedland v. Gales*, 131 N.C. App. 802, 806, 509 S.E.2d 793, 796 (1998) (citation omitted). "The essential elements of estoppel are (1) conduct . . . which amounts to a false representation or concealment of material facts; (2) the intention that such conduct will be acted on by the other party; and (3) knowledge, actual or constructive, of the real facts." *Id.* at 807, 509 S.E.2d at 796-97.

Azima alleges that Del Rosso concealed his involvement in the hacking, including his interactions with CyberRoot, beginning in at least August 2016 and continuing in 2020. Compl. ¶¶ 35, 36. Del Rosso (and others) sent false emails that were contradicted by other evidence and that were "an attempt to lay a false 'paper trail' of discovery." *Id.* ¶ 36. Del Rosso's fraudulent concealment continued through a false witness statement and false testimony in 2020. *Id.* ¶¶ 8, 36. Despite working diligently to identify the hackers, Azima did not learn of Defendants' role until after the May 2020 judgment in England. *Id.* ¶¶ 36, 127.

Because the Complaint alleges that Defendants and others intentionally and fraudulently concealed the facts giving rise to the Complaint, each statute of limitations

was tolled until August 2020. Accordingly, the motion to dismiss because of a statute of limitations defense must be denied.

B. Defendants Engaged in Actionable Conduct Within the Relevant Limitation Periods.

Putting aside Defendants' concealment, ten of the eleven counts are facially timely because of tortious acts in 2018 and 2019 and the discovery of the identity of the Defendants' role in 2020.

Statutes of limitations generally run from the date of the final tortious act needed to state an element of the offense. *Guessous v. Fairview Prop. Inv., LLC*, 828 F.3d 208, 222 (4th Cir. 2016); *Williams v. Blue Cross Blue Shield of N. Carolina*, 357 N.C. 170, 179, 581 S.E.2d 415, 423 (2003) (applying doctrine to state law). Other statutes of limitations do not run until the identity of the wrongdoer was discovered or reasonably should have been discovered. *See* N.C. Gen. Stat. §§ 14-113.20, 75-66, and 1-539.2C(c).

Defendants engaged in unlawful disclosure, use, and misappropriation of Azima's stolen data, including trade secrets, in May and June 2018 and June 2019. Compl. ¶¶ 24, 26. Therefore, the statutes of limitations for the eight counts where disclosure, use, misappropriation, unlawful copying, or transfer is an element – including Counts I and II (Wiretap Act), Counts III and VIII (Misappropriation of Trade Secrets), Count V (Conversion), Count IX (Unfair and Deceptive Trade Practices), Count X (Civil Conspiracy), and Count XI (Invasion of Privacy) – did not begin to run until after the last disclosure, use, or misappropriation in 2019.

The statutes of limitations for Counts VI (Identity Theft) and VII (Publication of Personal Information) did not begin to run until Azima learned of the Defendants' role in August 2020. Compl. ¶¶ 8, 36, 127.

Accordingly, these counts are facially timely even without Defendants' fraudulent concealment because of Defendants' tortious conduct in 2018-19 and the discovery of Defendants' role in 2020.

III. This Suit Is Not Precluded by an Ongoing English Lawsuit That Involves Different Parties.

Defendants contend that an ongoing breach of contract lawsuit, in a different country, involving different parties, different laws, and different claims precludes them from being sued. ECF No. 32 at 10-15. Defendants were not parties to that suit, which took place in England due to the contract's forum selection clause. *See id.* at 3-4. It was not alleged in that suit (and it was concealed at the time) that Defendants directed the hacking of Azima. Defendants cannot invoke as the basis for preclusion an ongoing English lawsuit in which they testified falsely to conceal their role.

Defendants have the burden of establishing an affirmative defense such as preclusion. *See*, *e.g.*, *United States v. Duke Energy Corp*., No 1:00CV1262, 2012 WL 1565228, at *3 (M.D.N.C. Apr. 30, 2012); *Allen v. Zurich Ins. Co*., 667 F.2d 1162, 1166 (4th Cir.1982) ("[T]his of course includes presenting an adequate record for the purpose."). Courts "narrowly construe" preclusion doctrines. *Nippon Shinyaku Co., Ltd. v. Iancu*, 369 F. Supp. 3d 226, 237 n.6 (D.D.C. 2019). Defendants cannot prevail on this argument under the Rule 12 standard.

"It is well-established that United States courts are not *obliged* to recognize judgments rendered by a foreign state, but may *choose* to give *res judicata* effect to foreign judgments on the basis of comity." *Gordon and Breach Sci. Publishers v. Am. Institute of Physics*, 905 F. Supp. 169, 178-79 (S.D.N.Y. 1995). "[I]t is primarily principles of fairness and reasonableness that should guide domestic courts in their preclusion determinations." *Id.*; *see also Andes v. Versant Corp*., 878 F.2d 147, 149 (4th Cir. 1989) ("The Full Faith and Credit Clause . . . does not apply to foreign judgments.").

It is thus discretionary as to whether this Court should invoke preclusion at all with respect to a foreign proceeding. Defendants' concealment alone, which must be taken as true at this stage, should suffice to prevent this Court from considering Defendants' preclusion defenses. But even if the Court were inclined to look past that concealment, there is still no proper ground for invoking preclusion here, particularly at this stage of the proceeding where the intricacies of the U.K. proceeding have not been established by Defendants with anything close to sufficient precision to establish the elements of preclusion. Simply put, neither the Complaint, nor any of the exhibits attached by Defendants, remotely support a finding that the claims in this case have been, or even could have been, litigated previously by these parties.

A. Defendants' Concealment of Facts from the English Court Bars Them from Arguing Preclusion.

Neither *res judicata* (claim preclusion) nor collateral estoppel (issue preclusion) applies when the defendant conceals or misrepresents evidence in an earlier proceeding, or when evidence was previously unavailable or undiscoverable prior to the earlier

proceeding. *Harnett v. Billman*, 800 F.2d 1308, 1313 (4th Cir. 1986) (noting "[a]n exception to the general principle that lack of knowledge will not avoid the application of *res judicata* rules" when "fraud, concealment, or misrepresentation have caused the plaintiff to fail to include a claim in a former action"); *see also United States v. Ruhbayan*, 325 F.3d 197, 204 (4th Cir. 2003) (holding party was not "afforded a full and fair opportunity to litigate the issue" because evidence was "unavailable and undiscoverable").

The Complaint alleges that Defendants and their co-conspirators concealed and misrepresented facts in the English proceeding about Defendants' role in the hacking and distribution of stolen data. Compl. ¶¶ 8, 34-36. That allegation must be taken as true and dooms Defendants premature maneuver to avoid discovery.

B. Azima's Claims are Not Barred by Claim Preclusion.

Claim preclusion applies only where there is "(1) a final judgment on the merits of the same claim in a prior suit; (2) an identity of the cause of action in both the earlier and the later suit; and (3) an identity of parties or their privies in the two suits." *SAS Inst., Inc. v. World Programming Ltd.*, 874 F.3d 370, 378 (4th Cir. 2017) (quotations omitted). Defendants have not established any of these elements, much less that all of them exist on the face of Azima's complaint. Claim preclusion is therefore inappropriate.

First, there is no prior final judgment in the ongoing English proceedings, and certainly no judgment that should be given preclusive effect here.[2] "A final judgment is one which disposes of the cause as to all the parties, *leaving nothing to be judicially*

[2] Defendants do not argue that the D.C. case has any preclusive effect.

determined between them in the trial court." *Forman v. U.S. Bank Nat. Ass'n*, No. 1:08CV287, 2008 WL 4287948, at *3 (M.D.N.C. Sept. 16, 2008) (emphasis added and quotations omitted). The English judgment Defendants rely upon is one where a witness recanted substantial testimony after the trial and the Court of Appeal criticized the judgment and accepted the discretionary appeal. Declaration of Ian Herbert, Exhibit 1. The Court of Appeal has ruled that Azima's appeal "do not appear to be without substance," that Azima's fresh evidence application "has a real prospect of success, and if successful it may put a new complexion on matters at least sufficient to justify a re-trial." *Id.*; *see also United States v. Al Fawwaz*, 116 F. Supp. 3d 194, 212 (S.D.N.Y. 2015) (noting English appeals are only granted with a real prospect of success or another compelling reason). It would be inappropriate to dismiss Azima's case based on the English proceedings where the Court of Appeals has so criticized the judgment of the trial court. That is particularly true where the trial court ruled that the true story of how RAKIA came into possession of Azima's data did not come out at trial, as discussed *infra* Section III.C, essentially inviting this suit.

Second, the Defendants have failed to demonstrate – and notably fail to even argue – that Azima could have raised these claims against them in England. Courts consider "whether the claim presented in the new litigation 'arises out of the same transaction or series of transactions as the claim resolved by the prior judgment'" and whether "the claims could have been brought in the earlier action." *SAS Inst., Inc.*, 874 F.3d at 378 (citation omitted). "When considering whether a prior action involved the same nucleus of facts for

preclusion purposes, [the Court] must narrowly construe the scope of that earlier action." *Nippon Shinyaku*, 369 F. Supp. 3d at 237.

The English proceeding was a breach of contract case with venue in England due to a forum selection clause. ECF No. 31-2 at 10, ¶ 43. Hacking was raised as a defense and counterclaim against RAKIA, primarily to bar RAKIA from using the stolen data and to dismiss the contract suit as an abuse of process. *Id.* at 12-13, ¶¶ 56-57. The counterclaim was stayed and never resolved on the merits. *Id.* at 12, ¶ 57. Moreover, Defendants fail to show if or how Azima could not have brought his claim against the Defendants in the English contract case. As a result, "[t]he fact that two suits involve challenges to very similar courses of conduct does not matter." *SAS Inst., Inc.,* 874 F.3d at 378 (noting "the U.S. suit alleged violations of U.S. copyright, which [the defendant] has not established could have been litigated in U.K. courts.").

Third, by their own admission, "Defendants were not parties in the English Proceedings," ECF No. 32 at 13, where *RAKIA* sued Azima, Compl. ¶ 7. Defendants rely upon *Lubrizol Corp. v. Exxon Corp*., 871 F.2d 1279, 1280 (5th Cir. 1989), for the proposition that "principal-agent relationships *may* ground a claim preclusion defense." ECF No. 32 at 13. The word "*may*" is important: Not even the attorney-client relationship automatically creates privity. Instead, privity centers on the closeness of the relationship. *Weinberger v. Tucker*, 510 F.3d 486, 493 (4th Cir. 2007). Defendants point to nothing in the record that demonstrates RAKIA was acting as Defendants' privy when it litigated the English case, or that the two were in privity in connection with the hacking. Indeed, the evidence suggests that the interests of RAKIA and the Defendants were not necessarily

aligned. RAKIA has claimed no knowledge of the hacking, ECF No. 31-2 at 106 – 116, meaning that it has affirmatively denied being in privity with those who conducted the hack. Claim preclusion does not apply here.

C. Azima's Claims Are Not Barred by Issue Preclusion.

Azima's claims are also not barred by issue preclusion. Issue preclusion bars relitigation of issues "'actually and necessarily determined by a court of competent jurisdiction' in the first litigation." *In re Varat Enterprises, Inc*., 81 F.3d 1310, 1315 (4th Cir. 1996).

First, the issues in the Complaint were never considered by the English Court. Nor did the English court resolve who was responsible for hacking Azima. The only hacking issue before the English court, raised primarily as a basis to exclude use of the stolen data in that case, concerned RAKIA's role in the hacking. ECF No. 31-2 at 80 - 85. The English court disbelieved RAKIA's story (which was supported by testimony from Del Rosso) that its agents innocently stumbled upon the stolen data on the internet; the court said that the true story of how RAKIA obtained Azima's data had not been revealed. Compl. ¶ 34. Defendants cannot use that ruling, which opens the door for this action, to prevent the true story from being revealed.

Second, the hacking issue at trial was governed by English law and rules of evidence. "[I]ssues are not identical if the second action involves the application of a different legal standard, even though the factual setting of both suits may be the same." *Yukos Capital S.A.R.L. v. OAO Samaraneftegaz*, 963 F. Supp. 2d 289, 295 (S.D.N.Y. 2013) (quoting *Peterson v. Clark Leasing Corp.*, 451 F.2d 1291, 1292 (9th Cir. 1971) and finding

no identity of issues when initial case governed by Russian Law and the second by U.S. law).

Third, even if the issue of Defendants' involvement in the hacking had been adjudicated in the English proceeding – which it was not – Azima was not given a fair chance to litigate the hacking issue there. English discovery rules are far more circumscribed than ours (*e.g.*, there are no depositions in English proceedings and third-party discovery is limited). *Cf. Gordan and Breach Science Publishers S.A. v. American Institute of Physics*, 905 F. Supp. 169, 179 (S.D.N.Y. 1995) (holding Swiss and German judgments had no preclusive effect based on six factors, including civil law procedural differences). Issue preclusion does not apply where parties are unable to introduce evidence that may affect the court's judgment. *Rye v. U.S. Steel Min. Co*., 856 F. Supp. 274, 279 (E.D. Va. 1994). "If significant new evidence is uncovered," "then it cannot be found that a party was afforded a full and fair opportunity to present his case in the absence of that evidence." *Ohio Valley Env't Coalition v. Fola Coal Co., LLC*., No. 2:17-3013, 2018 WL 1833215 at 11 (S.D.W. Va. Apr. 17, 2018) (quotations omitted); *Folmar v. Harris*, 650 F. App'x. 818, 821 (4th Cir. 2016) (unpub. op.).

IV. Counts I and II State Claims Under the Electronic Communications Privacy Act.

Defendants argue that (1) the ECPA does not apply extraterritorially, (2) there is no aiding and abetting liability for the ECPA, and (3) the complaint does not plead an "intercept." ECF No. 32 at 16-19. These arguments are without merit.

First, Defendants' conduct occurred in the United States. Compl. ¶ 11. Defendants are a U.S. citizen and entity located in North Carolina. *Id.* ¶ 41. Defendants were hired "in the United States" to investigate Azima (who resides in the United States), hack and steal his data (located in the United States) and use that data against Azima. *Id.* ¶¶ 2, 10. Where, as here, a defendant's conduct occurs in the United States, there is "no extraterritoriality that would bar the application" of the statute. *Huff v. Spaw*, 794 F.3d 543, 547 (6th Cir. 2015).

Second, Azima alleges that Defendants have primary liability under 18 U.S.C. § 2520 because they disclosed and endeavored to disclose, *see* Compl. ¶¶ 44-53, and used and endeavored to use, *see id.* ¶¶ 54-58, Azima's electronic communications in violation of 18 U.S.C. § 2511(1)(c) and (d). Defendants were "hired to target Azima and to obtain Azima's emails and confidential data, as well as for other purposes." *Id.* ¶ 15. Defendants were part of a plan to "target," "attack," and "go after" Azima. *Id.* ¶ 14. As part of that plan, the co-conspirators agreed to monitor the activities of Azima and use that information against him. *Id.* Azima's stolen data was "used by Defendants . . . in an attempt to ruin Azima's reputation and damage him financially." *Id.* ¶ 1. Defendants communicated with Dechert LLP about this work on a regular basis. *Id.* ¶ 13. Given these allegations, Azima has adequately pleaded that Defendants are liable under § 2520 through their violations of § 2511(1)(c) and (d). *Doe v. Smith*, 429 F.3d 706, 709 (7th Cir. 2005) (sending copies of

intercepted communications via email or otherwise through interstate means violates the act).[3]

Defendants argue that the 1986 amendment to § 2520 eliminated civil liability for procuring another person to intercept electronic communications. ECF No. 32 at 17. But courts have found that § 2520 still permits such a claim. *See*, *e.g.*, *Lonegan v. Hasty*, 436 F. Supp. 2d 419, 428 (E.D.N.Y. 2006) (concluding based on the text and legislative history that "both the person who actually intercepted the communications and the person who procured the interception have violated the Act, and the victim is authorized to sue any person or entity who engaged in that violation."); *Boseovski v. McCloud Healthcare Clinic, Inc.*, No. 2:16-CV-2491-DMC, 2020 WL 68578, at *5-6 (E.D. Cal. Jan. 7, 2020); *cf. Attkisson v. Holder*, 925 F.3d 606, 622 (4th Cir. 2019) (noting but not deciding the issue). Because Azima has pleaded that Defendants disclosed, endeavored to disclose, used, and endeavored to use Azima's intercepted data, the Court need not decide whether Defendants are also liable for procurement of the intercept. Azima has clearly pleaded sufficient facts, however, to proceed on that alternate theory of procurement liability as well.

Third, Azima has adequately pleaded that his electronic communications were "intercepted" within the meaning of §§ 2520 and 2511(1)(c) and (d). As alleged, "[t]he successful hack gave CyberRoot ***persistent access*** to Azima's computers and email

[3] These allegations sufficiently plead disclosure and use, but in his English witness statement, which is noted in the Complaint, Del Rosso admits to emailing links to Azima's intercepted data and flying with Azima's intercepted data for use against Azima. *See* ECF No. 25-3, ¶¶ 10, 14, 16.

accounts, and CyberRoot obtained ***real time access*** to Azima's emails." Compl. ¶ 6 (emphasis added); *see also id.* ¶¶ 16, 17, 51, 55.

Where communications are "immediately and instantaneously" copied and create access "in near real-time," such communications are "intercepted." *Luis v. Zang*, 833 F.3d 619, 631-32 (6th Cir. 2016); *see also United States v. Szymuszkiewicz*, 622 F.3d 701, 703 (7th Cir. 2010) (Microsoft Outlook rule "that directed Outlook to forward . . . all messages . . . received" was an "interception"); *Ctr. Law & Consulting, LLC v. Axiom Res. Mgmt., Inc.*, 456 F. Supp. 3d 765, 770 (E.D. Va. 2020) (automatic duplication is interception).

Defendants argue that manually logging into an email account does not constitute an interception. *See* ECF No. 32 at 18. The *Axiom Res. Mgmt*. court specifically distinguished real-time access like the kind Azima has pleaded from manually logging into an email account. 456 F. Supp. 3d at 770. The Defendants also incorrectly rely on *United States v. Steiger*, which quoted with approval a law review article in which the author concluded that real-time auto-forwarding or routing was interception. 318 F.3d 1039, 1050 (11th Cir. 2003) (quoting Jarrod J. White, E–Mail @Work.com: Employer Monitoring of Employee E–Mail, 48 Ala. L.Rev. 1079, 1083 (1997)). Azima has pleaded the type of real-time, persistent access that courts have regularly found to qualify as interception.

V. Count III States a Valid Trade Secrets Act Claim.

In moving to dismiss Count III, Defendants argue that (1) there is no DTSA action for conspiracy, (2) the complaint does not adequately allege trade secrets, (3) the complaint does not allege how the trade secrets were used in or intended for use in interstate or foreign

commerce, and (4) the misappropriation predated the enactment of the DTSA. Def. Mot. at 19-22. These arguments are also without merit.

First, Azima alleges that Defendants have primary liability because they engaged in "misappropriation" when they acquired, disclosed and used trade secrets without consent while knowing or having reason to know that the trade secrets were acquired by improper means since Defendants themselves hired the hackers. Compl. ¶¶ 18, 29-30. "Misappropriation" means acquisition, disclosure, or use of a trade secret of another with knowledge that the trade secret was improperly obtained. *Broidy Capital Mgmt. LLC v. Muzin*, No. 19-CV-0150 (DLF), 2020 WL 1536350, at *12 (D.D.C. Mar. 31, 2020) (citing 18 U.S.C. § 1839(5)(a)-(b)).

Second, "trade secrets" includes "all forms and types of financial, business, . . . [or] economic information,. . . including . . . plans, . . . formulas, . . . [or] methods," tangible or intangible, if "the owner thereof has taken reasonable measures to keep such information secret" and "the information derives independent economic value, actual or potential, from not being generally known." 18 U.S.C. § 1839(3)(a)-(b). Azima alleges that the computers and accounts that were hacked included "highly confidential business plans and proposals, research supporting those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships." Compl. ¶ 102. Though a plaintiff "need not plead with specificity what particular proprietary information was misappropriated," *DocMagic, Inc. v. Ellie Mae, Inc.*, 745 F. Supp. 2d 1119, 1145 (N.D. Cal. 2010), Azima's Complaint specifically describes price lists connected with supply contracts for food transport for U.S. troops in

Afghanistan. Compl. ¶¶ 18, 52, 108; *see also Accenture Global Services GMBH v. Guidewire Software Inc.*, 581 F. Supp. 2d 654, 663 n. 9 (D. Del. 2008) (noting a "basic description of the nature of [plaintiff's] trade secrets" was sufficient post-*Twombly*); *Broidy*, 2020 WL 1536350, at *12.

Third, among others, the price lists to supply food for U.S. troops in Afghanistan were used in, or intended for use in, interstate or foreign commerce. Compl. ¶¶ 52, 108.

Fourth, Azima alleged that Defendants continued to misappropriate Azima's data after the DTSA was enacted in May 2016. Defendants obtained persistent access to Azima's accounts and computers, which continued beyond May 2016. *Id.* ¶ 6, 16. And in 2018 and 2019, links to Azima's stolen data were modified. *Id.* ¶¶ 24, 26; *see also supra* Section I.

VI. Azima Has Properly Alleged State Claims.

A cursory review of Azima's Complaint shows that the North Carolina claims are sufficiently pled.

Computer Trespass. Azima alleges that Defendants and their co-conspirators "use[d] a computer . . . without authority" with the intent to "copy computer data," and has therefore stated a claim under N.C. Gen. Stat. § 14-458. Compl. ¶¶ 2, 3, 6, 17.

Conversion. The Complaint also adequately pleads conversion. "By taking a copy of the computer files, a tangible property albeit in electronic form, [Defendants] deprived [Plaintiffs] of the sole and exclusive dominion and control over the proprietary information." *Bridgetree v. Red F Marketing LLC*, No. 3:10-CV-00228-FDW-DSC, 2013 WL 443698, at *15 (W.D.N.C. Feb. 5, 2013). "That plaintiff did not destroy the data base

or exclude the defendant from its digitally stored material is of no moment." *Id.* at *14. Transferring data can also constitute conversion. *Volt Power, LLC v. Butts*, No. 7:19-CV-149-BO, 2020 WL 3979659, at *5 (E.D.N.C. Jul. 14, 2020).

Identify Theft. It is a felony when a person "knowingly obtains, possesses, or uses identifying information of another person, living or dead, with the intent to fraudulently represent that the person is the other person" for improper purposes." N.C. Gen. Stat. § 14-113.20. As alleged, "identifying information" includes "passwords," "electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names," and "any other numbers or information that can be used to access a person's financial resources." Compl. ¶ 88 (quoting N.C. Gen. Stat. § 14-113.20). Azima alleged that Defendants hacked his computer network to obtain Azima's passwords and other information "with the intent to fraudulently represent that Defendants were the Plaintiff for the purposes of obtaining materials of value, benefit, and advantage." *Id.* ¶ 87.

Publication of Personal Information. Defendants' claim that Azima failed to plead that "he previously objected to the disclosure of any such information or that Defendants had 'actual knowledge' of such an objection[.]" ECF No. 32 at 23-24. But Azima alleged that "Defendants published Azima's personal information on blog sites hosting WeTransfer links in May and June of 2018, and again in June 2019," Compl. ¶ 93, ***after*** Azima responded to the complaint in England by claiming his data was illegally hacked. ECF No. 31-2 at 13, ¶ 57.

North Carolina Trade Secrets Protection Act. Azima alleged that his hacked accounts included "highly confidential business plans and proposals, research supporting

those plans and proposals (including costs and service projections), information concerning business strategies and opportunities, and contacts for important business relationships," Compl. ¶ 102, including "confidential internal price lists relating to food transport for U.S. troops in Afghanistan." Compl. ¶¶ 52, 102, 18. Azima's claims are sufficient. *See Heska Corp. v. Qorvo US, Inc.,* No. 1:19CV1108, 2020 WL 5821078, at *9 (M.D.N.C. Sept. 30, 2020) ("While it appears Defendants may desire a more particularized description of what . . . Plaintiff asserts constitute trade secrets . . . [plaintiff's] allegations are sufficient to place Defendants on notice as to the trade secrets they are accused of misappropriating."); *ATI Indus. Automation, Inc. v. Applied Robotics, Inc.*, No. 1:09CV471, 2014 WL 2607364, at *3 (M.D.N.C. Jun. 11, 2014) (price and confidential customer lists constitute trade secrets); *DSM Dyneema, LLC v. Thagard*, No. 13 CVS 1686, 2014 WL 5317770, at *7 (N.C. Super. Oct. 17, 2014) ("'sufficient particularity' . . . does not require . . . every minute detail of . . . trade secrets down to the finest detail").

Unfair and Deceptive Trade Practices. Defendants claim that Azima failed to allege a claim for unfair and deceptive trade practices because (1) "he has not sufficiently alleged an 'unfair or deceptive act or practice' by Defendants or that any such act had 'the capacity or tendency to deceive the average consumer'"; (2) "a UDTP claim can arise only from commercial activities 'in or affecting commerce,' which Azima does not allege"; and (3) Azima "claims only that Defendants were engaged to hack him for purposes of litigation . . . which is not actionable." ECF No. 32 at 25. None of Defendants' arguments warrant dismissal.

First, "[t]o be actionable under the statute, conduct must be 'immoral, unethical, oppressive, unscrupulous, or substantially injurious.'" *Gilbane Bldg. Co. v. Fed. Reserve Bank of Richmond, Charlotte Branch*, 80 F.3d 895, 902 (4th Cir. 1996) (quoting *Branch Banking & Trust Co. v. Thompson*, 107 N.C. App. 53, 418 S.E.2d 694, 700 (1992)). "Acts are deceptive when they possess[] the tendency or capacity to mislead, or create[] the likelihood of deception." *Id.* Either unfairness or deceptiveness can bring conduct within the purview of the statute; an act need not be both unfair and deceptive." *Id.* at 903. Azima has alleged numerous unfair and deceptive acts, including phishing and spear phishing emails to gain unauthorized access to this email accounts, misappropriation of trade secrets, state and federal felonies, and distribution of unlawfully acquired emails and related computer data, each of which constitutes an unfair and deceptive trade practice. *See, e.g.*, *Med. Staffing Network, Inc. v. Ridgway,* 194 N.C. App. 649, 659, 670 S.E.2d 321, 329 (2009) ("A violation of the Trade Secrets Protection Act constitutes an unfair act or practice under N.C. Gen. Stat. § 75–1.1.")

Second, "in and affecting commerce" means "all business activities," and "business activities" means "the manner in which businesses conduct their regular, day-to-day activities, or affairs, such as the purchase and sale of goods, or whatever other activities the business regularly engages in and for which it is organized." *HAJMM Co. v. House of Raeford Farms, Inc.*, 328 N.C. 578, 594, 403 S.E.2d 483, 493 (1991). Azima alleged, among other things, that Del Rosso owns Vital and "Vital purports to provide investigative services." Compl. ¶ 11. Azima also alleged that Dechert LLP conspired with and hired Defendants, who worked with others to hack Azima's computer network to steal his trade

secrets, business communications, and business plans and proposals. *See, e.g.*, *id.* ¶¶ 18, 50, 52, 65.

Third, Defendants cannot escape liability for their wrongful acts by claiming they hacked Azima "for the purposes of litigation." In the case cited by Defendants, *Reichhold Chemicals, Inc. v. Goel*, 146 N.C. App. 137, 156, 555 S.E.2d 281, 293 (2001), there was "no indication that plaintiff undertook those acts for any trade related purpose other than preparation" for the lawsuit. *Id.* at 157, 555 S.E.2d at 293. The court concluded that actions limited to preparing to file a lawsuit were not an unfair trade practice. *Id.* Here, Azima has alleged a much broader scheme in which Defendants were paid and hired other co-conspirators to steal Azima's confidential information to harm him, his business, his reputation, and his community standing. Compl. ¶¶ 9, 53, 58, 135.

Invasion of Privacy – Offensive Intrusion Upon Seclusion. Intrusion upon seclusion is intentional intrusion, physically or otherwise that would be highly offensive to a reasonable person. *Hartford Cas. Ins. Co. v. Ted A. Greve & Associates, PA*, 742 Fed. App'x. 738, 741 (4th Cir. 2018). Such intrusions include "'eavesdropping by wiretapping or microphones, peering through windows, persistent telephoning, unauthorized prying into a bank account, and opening personal mail.'" *Tillet v. Onslow Mem'l Hosp., Inc.,* 215 N.C. App. 382, 384, 715 S.E.2d 538, 540 (2011) (citation omitted). Azima has alleged that Defendants conspired to intrude upon Azima's privacy by hacking his computer network, including his email accounts, and obtaining real-time, persistent access to his accounts. Compl. ¶ 6, 51. Defendants' hacking into Azima's email and other information is like (if not even more injurious than) the recognized intrusions of

eavesdropping, unauthorized prying into bank accounts, and opening personal mail. It is not like *Dishner v. Goneau*, 2017 WL 397878 (N.C. Super. Ct. 2017), cited by the Defendants, ECF No. 32 at 32-33, in which the plaintiff made only "generalized conclusion[s]" about violations of privacy.

Conspiracy. "If two or more persons conspire or agree to engage in an unlawful enterprise, each is liable for acts committed by any of them in furtherance of the common design and the manner or means used in executing the common design." *Newton v. Barth*, 248 N.C. App. 331, 343, 788 S.E.2d 653, 663 (2016). A civil conspiracy claim requires: "(1) a conspiracy, (2) wrongful acts done by certain of the alleged conspirators in furtherance of that conspiracy, and (3) injury as a result of that conspiracy." *Krawiec v. Manly*, 370 N.C. 602, 613-14, 811 S.E.2d 542, 550-51 (2018). A plaintiff may seek damages for civil conspiracy "where there is an underlying claim for unlawful conduct" and the plaintiff alleges "the agreement of two or more parties to carry out the conduct and injury resulting from that agreement." *Toomer v. Garrett*, 155 N.C. App. 462, 483, 574 S.E.2d 76, 92 (2002). Azima has alleged facts sufficient show a conspiracy between Defendants, Dechert LLP, CyberRoot, and other co-conspirators, *see* Compl. ¶¶ 1, 5, 6, 16, 19, 78, 79, 130-35, and is therefore allowed to seek damages for that conduct.

CONCLUSION

For the foregoing reasons, the Court should deny Defendants' Motion to Dismiss.

This, the 11th day of January, 2020.

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand
North Carolina Bar No. 22275
Christopher W. Jones
North Carolina Bar No. 27625
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com

MILLER & CHEVALIER CHARTERED

/s/ Kirby D. Behre
Kirby D. Behre
Brian A. Hill
Tim O'Toole
Ian Herbert
Calvin Lee
900 16th Street, NW
Washington, D.C. 20006
Telephone: (202) 626-5800
Fax: (202) 626-5801
Email: kbehre@milchev.com
bhill@milchev.com
totoole@milchev.com
iherbert@milchev.com
clee@milchev.com

CERTIFICATE OF WORD COUNT

I certify under Local Rule 7.3(d)(1) that the body of this brief, headings, and footnotes together contain 6,250 words or fewer, as reported by the word count feature in Microsoft Word 2016.

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand
North Carolina Bar No. 22275
Christopher W. Jones
North Carolina Bar No. 27625
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com

CERTIFICATE OF SERVICE

I certify that I caused this document to be electronically filed document with the Clerk of Court using the CM/ECF system, which will send electronic notification to all counsel of record:

NELSON MULLINS RILEY & SCARBOROUGH LLP

Kieran J. Shanahan, NCSB# 13329
Brandon S. Neuman, NCSB# 33590
Jeffrey M. Kelly, NCSB# 47269
Nathaniel J. Pencook, NCSB# 52339
GlenLake One
4140 Parklake Avenue, Suite 200
Raleigh, North Carolina, 27612
Telephone: (919) 329-3800
Facsimile: (919) 329-3799
kieran.shanahan@nelsonmullins.com
brandon.neuman@nelsonmullins.com
jeff.kelly@nelsonmullins.com
nate.pencook@nelsonmullins.com

Counsel for Defendants

Dated: January 11, 2021

WOMBLE BOND DICKINSON (US) LLP

/s/ Ripley Rand
Ripley Rand
North Carolina Bar No. 22275
Christopher W. Jones
North Carolina Bar No. 27625
555 Fayetteville Street, Suite 1100
Raleigh, North Carolina 27601
Phone: 919-755-2100
Fax: 919-755-2150
Email: chris.jones@wbd-us.com
ripley.rand@wbd-us.com